University of Essex

Online

Seminar Session – 1

Network Security
The Solar Winds Breach Case Study

(seminar is being recorded)

Beran Necat
beran.necat@kaplan.com

University of Essex

Online

Seminar Outline

- Announcements
- Cyber Kill Chain Model
- The Solar Winds Breach Case Study
- Assessment 1
- Q&A
- Further information

University of Essex

Online

Announcements

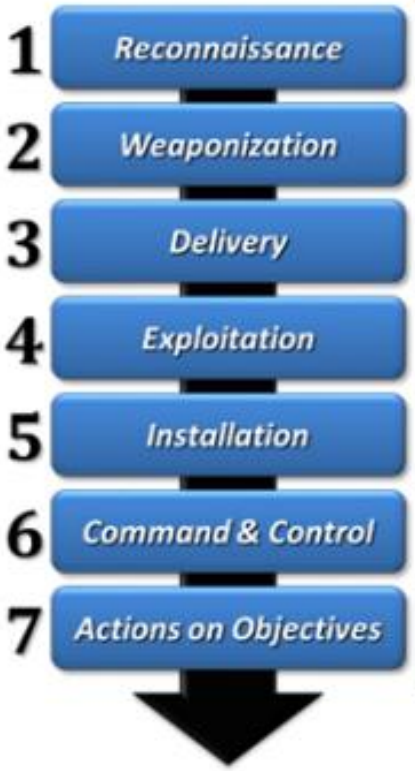
- Collaborative Discussion 1: Digitalisation
- Vulnerability Analysis – Literature Review Activity

University of Essex

Online

Cyber Kill Chain

- Lockheed Martin
- Widely adopted
- Some critiques



SOLARWINDS CYBER ATTACK

Reference: Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80.

University of Essex Online

The Solar Winds Breach Case Study

- Create a table that analyses the solar winds exploit using the Cyber Kill Chain. Are there any phases that you cannot identify?
- Create a list of possible mitigations for each phase. Are there any phases you cannot mitigate?
- What tools would you utilise in each phase? Give reasons for your answer.
- Create a slide deck presentation with up to 4 slides that discuss your solution. Be prepared to present it at the seminar this week.

University of Essex Online

Assessment 1

- Vulnerability Audit and Assessment - Baseline Analysis and Plan
- https://www.my-course.co.uk/mod/assign/view.php?id=661848
- Individual submission – Due end of Unit 3 – **600 Words**

- You have been assigned a website which will be assessed based on **academic research**

- You need to produce an analysis document for your client which covers the following requirements:

  Details of possible security vulnerabilities.

  A list of standards appropriate to their business and any non-compliance against those standards.

  A summary of recommendations and potential mitigations that could be used to ameliorate any risks. These should be ordered by importance.

  TABLES & BULLET LISTS SHOULD BE USED TO STAY WITHIN WORD LIMIT

University of Essex

Online

Assessment 1 Guidance

- **Assignment Checklist**

1. Bulleted/tabular list of security challenges (generic plus ones specific to the business).
2. Bulleted/tabular list of the tools you will use (as well as your justifications, matching them against challenges).
3. Methodology (remote or local, automated or manual, etc.).
4. Discussion on the available models/methodologies/tools and approaches.
5. Selection of methods/tools/approaches.
6. Business impacts on use of tools and methods (scanning in or out of hours, traffic).
7. Timeline of the completion of the task.

University of Essex

Online

Next Week: Upcoming Seminar

- Unit 4 Seminar - Breach Analysis Case Study

- Read Swinhoe, D., 2020. The 15 Biggest Data Breaches of the 21st Century.

University of Essex

Online

Thank You

- Any Questions?